

# Compliance or Security, What Cost? (Poster)

Craig Wright

Springer-Verlag, Computer Science Editorial, Tiergartenstr. 17,  
69121 Heidelberg, Germany  
{cwright20}@postoffice.csu.edu.au

**Abstract.** This paper presents ongoing work toward measuring the effectiveness of audit and assessment as an information security control. The trend towards the application of security control measures which are employed to demonstrate compliance with legislation or regulations, rather than to actually detect or prevent breaches occurring is demonstrated to result in a misallocation of funds. Information security is a risk function. Paying for too much security can be more damaging in economic terms than not buying enough. This research reveals several major misconceptions among businesses about what security really means and that compliance is pursued to the detriment of security. In this paper, we look at some of the causes of compliance based audit failures and why these occur. It is easier to measure compliance than it is to measure security and spending money to demonstrate compliance does not in itself provide security. When the money spent on achieving compliance reduces the funding available for control measures that may actually improve security problems may arise.

**Keywords:** Audit, Economics, Incentives, Risk, Security, Compliance.

## 1 Introduction

Information security is a risk function [1]. Paying for too much security can be more damaging in economic terms than not buying enough. This paper presents ongoing work toward measuring the effectiveness of audit and assessment as an information security control. In this paper, we demonstrate that the trend towards the application of security control measures which are employed to express compliance with legislation or regulations, rather than to actually detect or prevent breaches occurring results in a misallocation of funds. Information security is a risk function. Paying for too much security can be more damaging in economic terms than not buying enough. This research reveals several major misconceptions among businesses about what security really means and that compliance is pursued to the detriment of security. In this paper, we look at some of the causes of compliance based audit failures and why these occur. The major point of the paper is that it is easier to measure compliance than it is to measure security, and that spending money to demonstrate compliance does not in itself provide security.

This extends to include a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in

order to provide compliance with little true economic gain. Funds are moved to alternate uses with no further funds allocated.

This paper presents the early research into an empirical study of data collected by the authors from 2,361 information systems audits in the period 1998 to 2010. These audit reports were collected from 894 Australian and US organizations in the Finance, Gaming, Media, FMCG, and Mining sectors as well as both Federal and State Government departments. Reports from Chartered audit firms, security companies and internal audit contractors are included. The composition of Australian organizations varies greatly. All US organizations consist of medium or larger listed companies with requirements under the Sarbanes Oxley Act (Sect 3.2 & 404). The audit reports from Australian organizations include PCI-DSS, APRA, BASELII, AML-CTF and those required for listed company financial reporting. This research incorporated the financial data for 451 of the organizations. An analysis of 210 incidents that resulted in a compromise will be analyzed in a forthcoming examination.

## 2 Misaligned Incentives: Audit and the Failure to Determine Risk

The existing audit industry provides compliance services under the guise of security. These services provide little if any increase in security and yet consumers purchase them. In addition, it is demonstrable that these services are extremely inelastic for large organizations<sup>1</sup>. There are several reasons for this. First, government<sup>2</sup> or commercial groups (e.g. PCI-DSS) mandate many compliance regimes. Next, negligence rules and the governance functions of companies require that boards and senior management take action to protect the value of the company. Unfortunately, this also means using reports that demonstrate compliance from audit companies in place of a real effort to ensure that data protection occurs.

In a review of 1,878 audit and risk reports collected by the authors on Australian firms by the top 8 international audit and accounting firms, 29.8% of tests evaluated the effectiveness of the control process. The security of systems were validated to any level in only 6.5% of reports. Of these, the process rarely tested for effectiveness, but instead tested that the controls met the documented process. Audit practice in US and UK based audit firms does not differ significantly.

Installation guidelines provided by the Centre for Internet Security (CIS)<sup>3</sup> openly provide system benchmarks and scoring tools that contain the “*consensus minimum due care security configuration recommendations*” for the most widely deployed operating systems and applications in use. The baseline templates will not themselves stop a determined attacker, but can to demonstrate minimum due care and diligence. Only 32 of 542 organizations analyzed in this paper deploy this form of implementation standards.

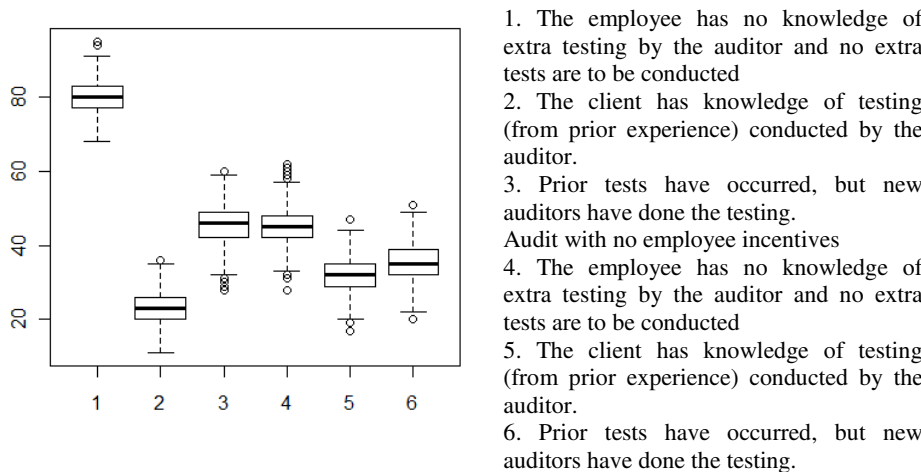
---

<sup>1</sup> Although these services may remain highly elastic for many smaller organizations who may choose not to control risk when budgets are tight.

<sup>2</sup> This includes SOX, APRA, FISMA, and many other compliance regimes.

<sup>3</sup> CIS benchmark and scoring tools are available from <http://www.cisecurity.org/>

The information systems employees within an organization also have a misaligned set of incentives. A large component of any audit involves discussions with the employees and management at the examined organization. The term auditor essentially derives from the act of listening as '*one who listens*'. Listening to the assertions of employees remains a large component of any information systems audit. Those interviewed in this process include the employees who are responsible for the maintenance of the system audited. These same employees commonly have incentives that align with the audit results. For instance, in 1,325 of the audits review that directly include firewalls, 798 (60.2%) of these audits involved direct interviews with firewall administrators who either had bonuses tied to the outcome of the audit or whose employment was in some manner conditional on the outcome of the audit.



**Fig. 1.** Misaligned incentives and a lack of accuracy delivered to the auditor (%) in an audit with employee incentives

The consequence of these misaligned incentives is obvious, misinformation. Fig. 1 displays the results of the audit when the employee has incentives and knowledge or neither. Further analysis associated to the assignment of a new auditor followed. The differences between the audits of a known tested system known and of a system excluded from testing were statistically significant at the  $\alpha = 5\%$  level. At this level, we have a confidence interval of (77, 83) with a corresponding confidence interval of (20, 26) when the employee has incentives and knows that the statements they offer will be tested. The distinction from an employee with incentives who has been audited and had their assertions validated (42, 48) when a new auditor is assigned do not differ significantly from the employee with no incentives (42, 49).

### 2.1 Patching and Validation

Patching is a common test for compliance. Auditors assert that this compliance test aligns to good security practice [5]. A correctly patched system is less likely to

experience issues and be more secure [2]. This is agreed. The question is what is "correctly patched" and "have the patches been applied correctly"? Audits generally test for the application of patches. The problem is that this is generally limited to testing the existence of operating system that has all required patches applied. Application patches are another matter.

Tests of the patching processes for Windows Servers, clients, applications, routers, switches and firewalls are reported in Table 1. The 95% confidence intervals for patching times for each of these systems have been recorded. The patch date is determined as the difference in time between when the software vendor has released the patch to the installation of the patch on the system. In a few instances, this result is statistically censored due to the lack of patching. This can take place where the system is installed and left running without the application of updates. In this case, the difference between the installation date of the device and the date of the patch or update that should be applied is used to determine the interval. This situation was found to be most common in network equipment (with several routers and switches never having been patched or updated) as well as with selected examples of user application software.

**Table 1.** Patching Analysis of Audited Systems

	No. Analyzed	95% Confidence Interval of days between patching (Mean)	Average Policy Patch time (CI)	% Prior Reports noting patching
Windows Server	1571	41.1, 122.4 (86.2)	55.5, 87.9	98.4%
Windows Client	13,951	22.8, 69.3 (48.1)	29.6, 49.4	96.6%
Other Windows Applications	30,290	58.1, 181.8 (125.2)	68.1% NA	18.15%
Internet Facing Routers	515	58.2, 164.1 (114.2)	58.1% NA	8.7%
Internal Routers	1,323	129.3, 384.6 (267.8)	73.2 NA	3.99%
Internal Switches	452	139.9, 483.9 (341.2)	87.5 NA	1.2%
Firewalls	1,562	21.5, 65.7 (45.4)	24.5, 108.2	70.7%

A further analysis of prior audit reports was conducted to note how many of these had included patch levels for each of the various hosts and systems deployed at the audited client. Nearly all audit reports note the inclusion or exclusion of operating system patches (98.4% and 96.6% for server and client systems respectively). The majority of these reports included no testing of the network devices and little tests of the application software in use by a client. Network switches were the least analyzed device. The mean time between patching on these devices was recorded at 341.2 days. It was uncommon for organizations to have a policy requiring the patching of network devices. The majority of organizations have policies in place for the patching of Servers (with a range of 55.5 to 87.9 days) and Client operating systems (with a range of 29.6 to 49.4 days). All results and Confidence intervals are reported at a 95% CI.

Operating system patches for client systems and firewalls are generally applied and tested within 60 days. The patching rates for network equipment vary significantly. Again, it is clear that the incentives to ensure compliance result in insecure systems. The audit process checked policy statements against a sample of systems, but did nothing to validate those systems not included in the policy. The result is an overwhelming focus on selected systems that are incorporated within a checklist at the expense of excluding many essential systems.

The patching of client applications was problematic with a mean of 125.2 days between patching of these applications and a 95% confidence interval of (58.1, 181.8) days. This varied widely not only across hosts and organizations, but also within the same host. Only 2.18% of hosts have patched at least 95% of applications within 120 days. The development systems analyzed exhibited the worst results. Compilers and IDE (integrated development software) were patched at a rate of between (82.0, 217.3) days. These systems were also generally not included within the audit report. The consequence being that there is little incentive for the organization to ensure that they are maintained sufficiently.

## 4 Conclusion

Compliance is easier than security. It would seem costs of normal compliance auditing do not benefit the bottom line financial posture of organizations seeking to be both secure and compliant. An appropriate view would be to seek to be secure in place of appearing secure. This leads to an endless cycle of continual audit satisfying the needs of compliance and the bottom lines of financial firms, but with few other true paybacks. So we are led to ask, at what cost?

The practice of implementing monitoring controls that do not report on breaches, but which do satisfy the compliance needs of an organization can cost far more in the long term [1,3]. Businesses need to demand more thorough audits and results that are more than simply meeting a compliance checklist. These must include not only patching for all levels of software (both system and applications) as well as the hardware these run on. This failure of audits to "*think outside the box*" and only act as a watchdog could ultimately be perceived as negligence for all parties.

Compliance at the expense of security in the global economy is a practice that is difficult to overcome, but a challenge that we have to meet. It may be easier to measure compliance than it is to measure security, but spending money to demonstrate compliance does not in itself provide security. When the money spent on achieving compliance reduces the funding available for control measures that may actually improve security problems may arise.

## References

1. Anderson, R.: Why information security is hard – an economic perspective. In: 17th Annual Computer Security Applications Conference, pp. 358–365 (2001)
2. Halderman, J.: To Strengthen Security, Change Developers' Incentives. IEEE Security and Privacy 8(2), 79–82 (2010)
3. Katz, M.L., Shapiro, C.: Network externalities, competition, and compatibility. The American Economic Review 75, 424 (1985)
4. Roesse, N.J., Olson, J.M.: Better, stronger, faster: Self-serving judgment, affect regulation, and the optimal vigilance hypothesis. Perspectives on Psychological Science 2, 124–141 (2007)
5. Turcato, L.M.: Use of COBIT as a Risk Management & Audit Framework for Access Compliance, San Francisco ISACA Fall Conference (2004)